Mobile Messenger Security Report

July 2017

Official Disclaimer

This report prepared by Solared Cyber Security is based on the results of instant messenger research and functionality testing and is for information purposes only.

The research findings specified in the report were obtained through automatic binary analysis and without reverse engineering (i.e. source code decompilation).

Any other information herein was obtained from sources considered reliable by Solared Cyber Security. However, the company does not guarantee information accuracy and completeness for any purpose.

Trademarks mentioned herein are the property of their respective owners.

No information specified in this report may be interpreted (directly or indirectly) as containing Solared Cyber Security's investment or software use recommendations. Any results herein are valid on the date of publication and may be changed without prior notice.

Solared Cyber Security shall not be held liable for any loss or damage caused by the use of information herein by any third party, including published opinions or conclusions, or for any consequences related to the provision of incomplete or inaccurate information.

Methodology

The security research involved the comparison of popular free mobile messengers: Facebook Messenger®, QQ International™, Signal™, Skype™, Slack®, Telegram®, Viber®, WeChat®, and WhatsApp®, each of which was studied in both iOS® and Android™ versions.

Code security was assessed automatically using SolaredAPPscreener, a software product for static, dynamic, and interactive analysis, without app decompilation or deobfuscation. Binary code static analysis was performed automatically and without human interference. As a result, any conclusions based on automatic analysis do not reflect report's authors' opinion.

Following the app analysis, SolaredAPPscreener generated reports containing an overall security score on a scale from one to five and a list of revealed backdoors, vulnerabilities and errors ranked by severity. These reports formed the basis of the research.

App security score was calculated automatically and based on how many and how often various types of critical and mid-level vulnerabilities appeared in a code. The number of critical vulnerabilities, regardless of code size, contributed more to the score than mid-level vulnerabilities being adjusted in line with code size.

Based on the most recent 500 scans, SolaredAPPscreener calculated an industry average app security level of 1.6 points on the day of the report.

1 Facebook Messengers for iOS v. 122.0; Facebook Messengers for Android v. 124.0.0.43.69.
2 QQ International for iOS v. 4.8.4; QQ International for Android v. 5.2.0.
3 Signal for iOS v. 2.12.2; Signal for Android v. 4.7.4.
4 Skype for iOS v. 6.35.1; Skype for Android v. 7.46.0.596.
5 Slack for iOS v. 2.6.2; Slack for Android v. 2.37.0.
6 Telegram for iOS v. 4.0; Telegram for Android v. 4.1.
7 Viber for iOS v. 6.9.5; Viber for Android v. 7.1.0.6.
8 WeChat for iOS v. 6.5.9; WeChat for Android v. 6.5.8.
9 WhatsApp for iOS v. 2.17.31; WhatsApp for Android v. 2.17.223.

Introduction

Solared Cyber Security, a vendor of cybersecurity management and target monitoring products and services, has compared the most common iOS and Android messengers in terms of security. The company selected messengers with the highest number of monthly active users (MAUs).

As a result, we chose WhatsApp with around 1.2 billion MAUs, Facebook Messenger (around 1.2 billion), QQ International and WeChat (899 million and 806 million respectively). Moreover, the research featured Skype (300 million MAUs), Viber (260 million) and Slack (4 million active users per day). Finally, we included messengers which are claimed by their creators to be the most secure on the market: Telegram with around 100 million users and Signal. We did not find any accurate statistics on how popular Signal is, but decided that we could not ignore an app praised by Edward Snowden and Bruce Schneier.

When researching messenger security, mobile apps are often only assessed in terms of user data security. This report represents a comprehensive research of various messenger security threats, from user data interception to app vulnerability to a variety of attacks and known exploits.

Revealed Errors and Potential Vulnerabilities

Scanning revealed that the most common critical vulnerabilities in Android apps were weak hashing and encryption algorithms, empty passwords and insecurity of both SSL implementations and padding algorithms. All these vulnerabilities may be divided into two categories by a way they are exploited:

1. **Vulnerabilities that weaken the security of data being stored** and processed. Weak hashing and encryption algorithms and non-resilient encryption algorithm parameters increase the risk of compromising information stored on a device (user names, passwords, messages, etc.) and are usually exploited by malware (universal Trojan harvesters or app-specific Trojans).

2. **Vulnerabilities that allow for a Man-in-the-Middle attack.** In the event of insecure SSL implementation (empty method), an app does not check all certificate parameters when making a secure connection, thus increasing the risk of certificate spoofing and interception of data transmitted via a messenger. Such vulnerability may be easily exploited through a public Wi-Fi network, when the entire traffic between a victim's messenger and a server is routed via an attacker.

The same vulnerabilities, such as weak hashing and encryption algorithms and insecure SSL implementation (also when using AFNetworking library), are typical for iOS messengers. Unlike Android, iOS apps are not so exposed to the first category of vulnerabilities, unless iOS Jailbreaking is used.

Messenger Security:
Comparative Analysis Results

Android App Security Level:

Messenger	Critical vulnerabilities	Mid-level vulnerabilities	Low-level vulnerabilities	Overall security level
WhatsApp	0	24	12	4.4 / 5.0
Slack	3	256	736	2.7 / 5.0
Facebook Messenger	7	298	245	1.9 / 5.0
Viber	12	334	595	1.5 / 5.0
Telegram	16	293	641	1.3 / 5.0
Signal	19	437	649	1.1 / 5.0
Skype	18	348	537	1.1 / 5.0
QQ International	45	1085	1239	0.4 / 5.0
WeChat	54	1138	782	0.3 / 5.0

The table shows that WhatsApp is far ahead of its competitors in terms of security (4.4 out of 5 points), with the app receiving an extremely high score. The absence of critical vulnerabilities makes WhatsApp particularly secure, both in terms of user data protection and resilience to Trojan attacks or known exploits.

Even though Slack, Facebook Messenger, Viber, Telegram, Signal and Skype running under Android had a similar set of vulnerabilities, Slack faced fewer than other apps, receiving 2.7 points. On the other hand, QQ International and WeChat (both by Tencent Holdings Ltd.), turned out to have the largest number of vulnerabilities.

Messenger Security:
Comparative Analysis Results

iOS App Security Level:

Messenger	Critical vulnerabilities	Mid-level vulnerabilities	Low-level vulnerabilities	Overall security level
Signal	13	122	0	1.5 / 5.0
Slack	14	594	0	1.3 / 5.0
Skype	17	446	0	1.2 / 5.0
Facebook Messenger	18	436	0	1.1 / 5.0
WhatsApp	18	436	0	1.1 / 5.0
Viber	30	1025	0	0.7 / 5.0
Telegram	71	666	0	0.2 / 5.0
QQ International	891	2553	0	0 / 5.0
WeChat	1655	2685	0	0 / 5.0

The table shows that Signal, Skype, Slack, Facebook Messenger and WhatsApp received almost the same score with Signal and Slack remaining the leaders in terms of security (1.5 and 1.3 points respectively). QQ International and WeChat on iOS, once again, proved to be the least secure messengers with the largest number of revealed vulnerabilities.

The same messengers on iOS devices had more vulnerabilities compared to their Android equivalents, both by type and occurrence frequency.

Conclusions

Android messengers were found to be more secure than their iOS siblings, with the top three Android and iOS apps recording an average score of 3.0 and 1.3 points respectively.

The most common vulnerabilities are insecure SSL implementation and weak hashing and encryption algorithms, with successful exploitation having the potential to compromise user names, passwords and communications. While exploitation is not always easy, messengers that claim to be highly secure should take any potential threats seriously.

The top three most secure Android apps are WhatsApp, Slack and Facebook Messenger, with WhatsApp, receiving a particularly high score. Facebook Messenger and Slack also offer high code quality, while the latter is positioned as a corporate messenger and is officially the fastest growing business app of all time.

iOS leaders are Signal, Slack and Skype, all of which received very few security points, with Facebook Messenger and WhatsApp snapping at their heels.

Finally, QQ International and WeChat turned out to be the least secure apps, regardless of OS.